In the Claims:

Please amend claims 3, 5, 7-10, 12-15, 20, and 22-23. The claims are are as follows.

1. (Original) A method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, the method comprising the steps of:

encrypting the data item,

encrypting the one or more conditions separately from the data item, combining the encrypted data item and the encrypted one or more conditions, and

encrypting the combination to generate a digital signature block that inherently represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions.

2. (Original) A method according to claim 1, wherein each of a plurality of specified conditions is separately encrypted and combined with the encrypted data item, and wherein the combination is then further encrypted.

3. (Currently Amended) A method according to claim 1 ~~or claim 2~~, wherein the encryption of the data item and separate encryption of the conditions are each one-way hashing steps to generate verifiable representations of the data item and conditions.

4. (Original) A method according to claim 3, wherein the step of combining the hashed data item and conditions comprises concatenating the hashed data item and hashed conditions, hashing the product of the concatenation to produce a final digest, and further encrypting the final digest to generate a digital signature block.

5. (Currently Amended) A method according to claim 1 ~~or claim 2~~, wherein the step of encrypting the combination uses an encryption method for which the result of (a) combining the encrypted data item and the encrypted one or more conditions and then encrypting the combination differs from a result of (b) encrypting both the encrypted data item and the encrypted one or more conditions and then combining the doubly encrypted data item and conditions.

6. (Original) A method according to claim 5, wherein the encryption method implements Cipher Block Chaining encryption.

7. (Currently Amended) A method according to claim 1 ~~or claim 2~~, wherein the encryption of the data item and separate encryption of the conditions each use Cipher Block Chaining encryption methods.

8. (Currently Amended) A method according to ~~any one of the preceding~~ claim[[s]] 1, wherein the step of encrypting the combination to generate a digital signature block uses a private key of a public/private key cryptographic solution to produce a conditional signature.

9. (Currently Amended) A method according to ~~any one of~~ claim[[s]] 1 ~~to 7~~, wherein the step of encrypting the combination to generate a digital signature block uses a symmetric key of a symmetric-key cryptographic solution to produce a conditional signature.

10. (Currently Amended) A method according to ~~any one of the preceding~~ claim[[s]] 1, including the step of transmitting to a recipient the data item, the one or more conditions and the digital signature block, such that a recipient, who has access to the cryptographic processes used for performing the encrypting steps and has access to a corresponding decryption key, is enabled to:

decrypt the digital signature block to produce a first result;

encrypt the data item, encrypt the one or more conditions separately from the data item, and combine the encrypted data item and encrypted one or more conditions to produce a second result; and

compare the first and second results to determine whether they match.

11. (Original) A method according to claim 10, including transmitting the encryption algorithms to the recipient.

12. (Currently Amended) A method according to claim 10 ~~or claim 11~~, including transmitting to the recipient the interim results of each encryption step, comprising:

the encrypted data item; and

the encrypted one or more conditions.

13. (Currently Amended) A method according to ~~any one of~~ claim[[s]] 10 ~~to 12~~, wherein the step of encrypting the combination to produce a digitally signed data block uses a private key of a public/private key cryptographic solution, and wherein the method includes transmitting to the recipient the public key of the cryptographic solution.

14. (Currently Amended) A method according to ~~any one of~~ claim[[s]] 10 ~~to 12~~, wherein the step of encrypting the combination to produce a digitally signed data block uses a private key of a public/private key cryptographic solution, and wherein the method includes transmitting to the recipient information for obtaining the public key of the cryptographic solution.

15. (Currently Amended) A method according to ~~any one of~~ claim[[s]] 10 ~~to 14~~, including compiling a set of encryption results which set includes the results of each step of encrypting, and wherein the step of transmitting includes the step of transmitting the set of encryption results to the recipient.

16. (Original) A method according to claim 3, including the step of transmitting to a recipient the hashed representations of the data item and conditions and the digital signature block such that a recipient, who has access to the cryptographic process used to perform the step of encrypting the combination and has access to a corresponding decryption key, is enabled to:

decrypt the digital signature block;

combine the hashed representations of the data item and conditions to generate a combined digest; and

compare the decrypted signature block with the combined digest to determine whether they match.

17. (Original) A method according to claim 16, wherein the step of combining the hashed representations to generate a combined digest comprises the steps of:

concatenating the hashed representations to generate a double digest; and

hashing the double digest to generate a final combined digest.

18. (Original) A method according to claim 1, wherein each of a plurality of data items is separately encrypted and combined, and the combination is then further encrypted.

19. (Original) A method for verifying a conditional electronic signature, generated by a method according to claim 10, comprising the following steps performed in response to receipt by the recipient of the transmitted data item, one or more conditions and the digital signature block:

decrypting the digital signature block to produce a first result;

encrypting the data item, encrypting the one or more conditions separately from the data item, and combining the encrypted data item and encrypted one or more conditions to produce a second result; and

comparing the first and second results to determine whether they match.

20. (Currently Amended) A computer program product loadable into the internal memory of a digital computer, comprising software code portions for performing, when said product is run on

a computer, to carry out the invention of claim[[s]] 1 ~~to 18~~.

21. (Original) A computer program product loadable into the internal memory of a digital computer, comprising software code portions for performing, when said product is run on a computer, to carry out the invention of claim 19.

22. (Currently Amended) A data processing apparatus for generating conditional electronic signatures, comprising:

one or more cryptographic components, responsive to one or more conditions ~~(20)~~ being specified for an electronic signature of a data item ~~(10)~~, for encrypting the data item ~~(50)~~, encrypting ~~(50)~~ the one or more conditions separately from the data item, combining ~~(60)~~ the encrypted data item and the encrypted one or more conditions, and encrypting the combination to generate a digital signature block ~~(110)~~ that inherently represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions; and

means for transmitting to a recipient the data item, the one or more conditions and the digital signature block ~~(110)~~.

23. (Currently Amended) A data processing apparatus for verifying a conditional electronic signature, generated by a method according to claim 10, comprising:

means for receiving the transmitted data item, one or more conditions and the digital signature block ~~(110)~~; and

one or more cryptographic components for: decrypting the digital signature block to produce a first result; encrypting the data item, encrypting the one or more conditions separately from the data item, and combining the encrypted data item and encrypted one or more conditions to produce a second result; and comparing the first and second results to determine whether they match.

24. (Original) A method for disseminating status information for conditionally signed data items, wherein the conditionally signed data items include executable content for updating a registry in response to one of the conditionally signed data items being forwarded to a recipient or being identified as rejected, the registry maintaining a list of recipients of the data item, the method including the steps of:

in response to forwarding of the conditionally signed data item to a new recipient, executing the executable content to update the list of recipients in the registry; and

in response to an indication that the conditionally signed data item is rejected, executing the executable content to update the registry and disseminating an indication that the data item is rejected to each of the recipients in the registry list.

25. (Original) A data processing apparatus for disseminating status information for conditionally signed data items, comprising:

a registry for maintaining a list of recipients of a conditionally signed data item;

means for recognizing the presence of an executable component within a conditionally signed data item and, responsive to the data item being forwarded to a new recipient, for

initiating execution of the executable component to update the list of recipients within the registry; and

means, responsive to an indication that the data item is rejected, for updating the registry to indicate the rejection and for disseminating an indication that the data item is rejected to each of the recipients in the list.

26. (Original) A computer program comprising program code instructions for controlling the operation of a data processing apparatus on which the program code executes, to perform a method according to claim 24.